EP 1 821 457 A1

Fig.1

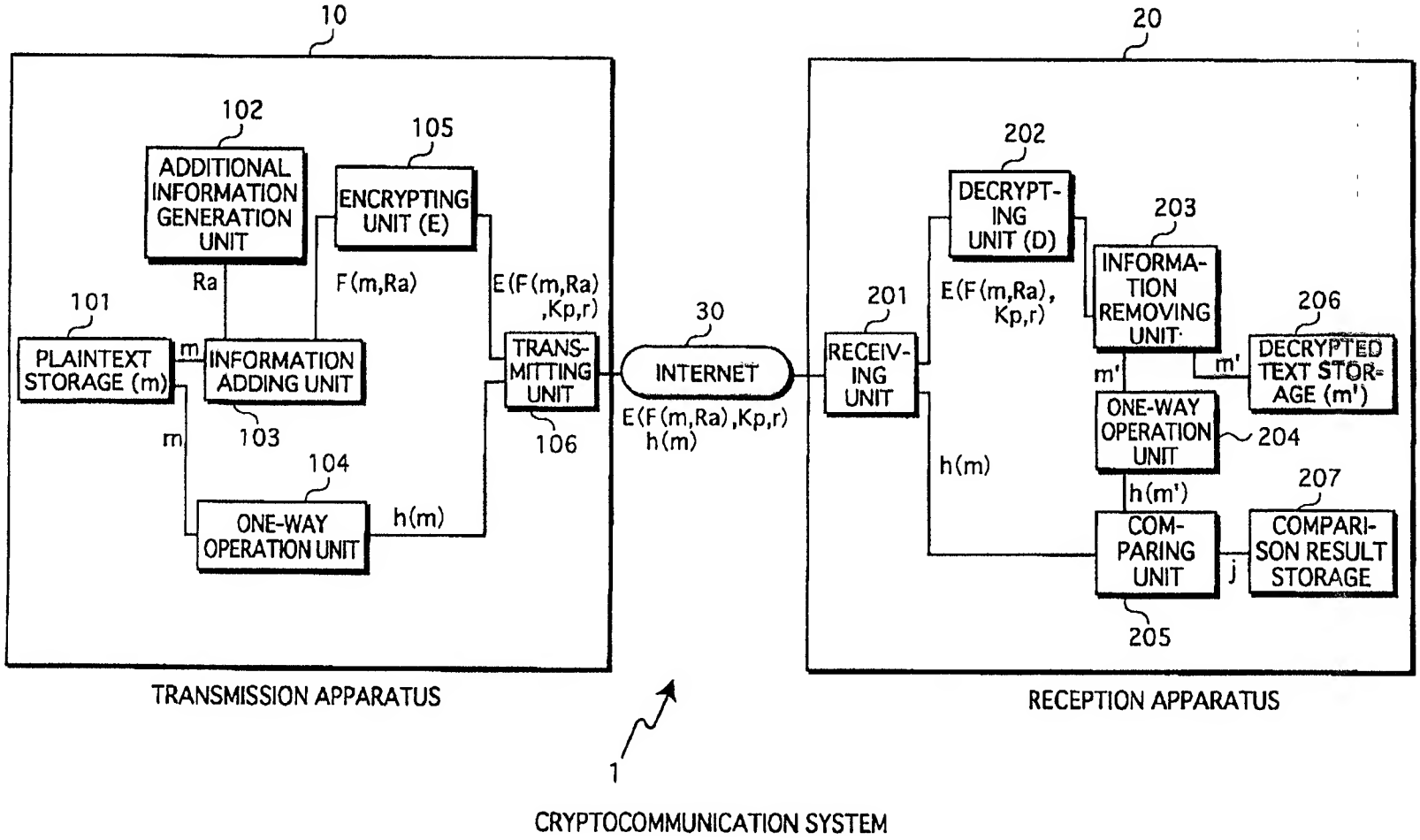


Fig.2

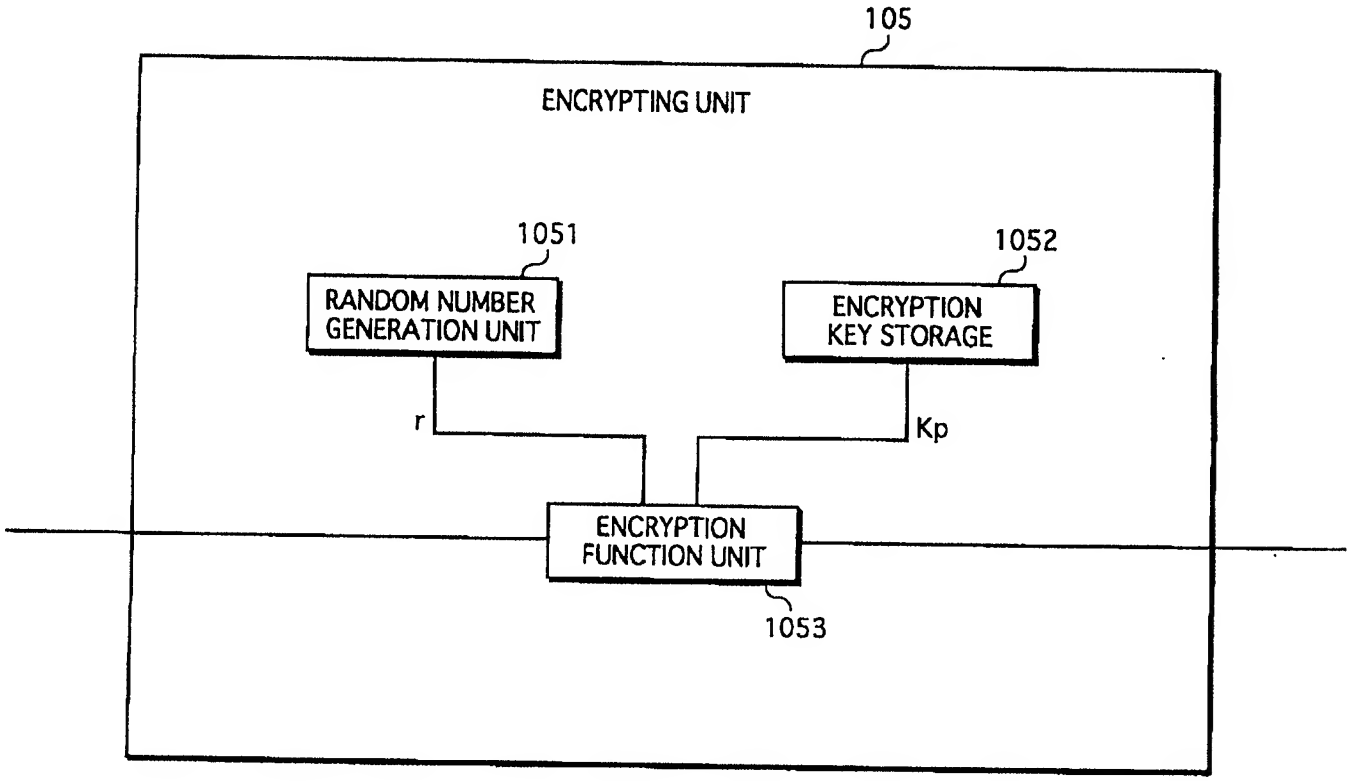

105
ENCRYPTING UNIT
1051
RANDOM NUMBER GENERATION UNIT
1052
ENCRYPTION KEY STORAGE
r
Kp
ENCRYPTION FUNCTION UNIT
1053

Fig.3

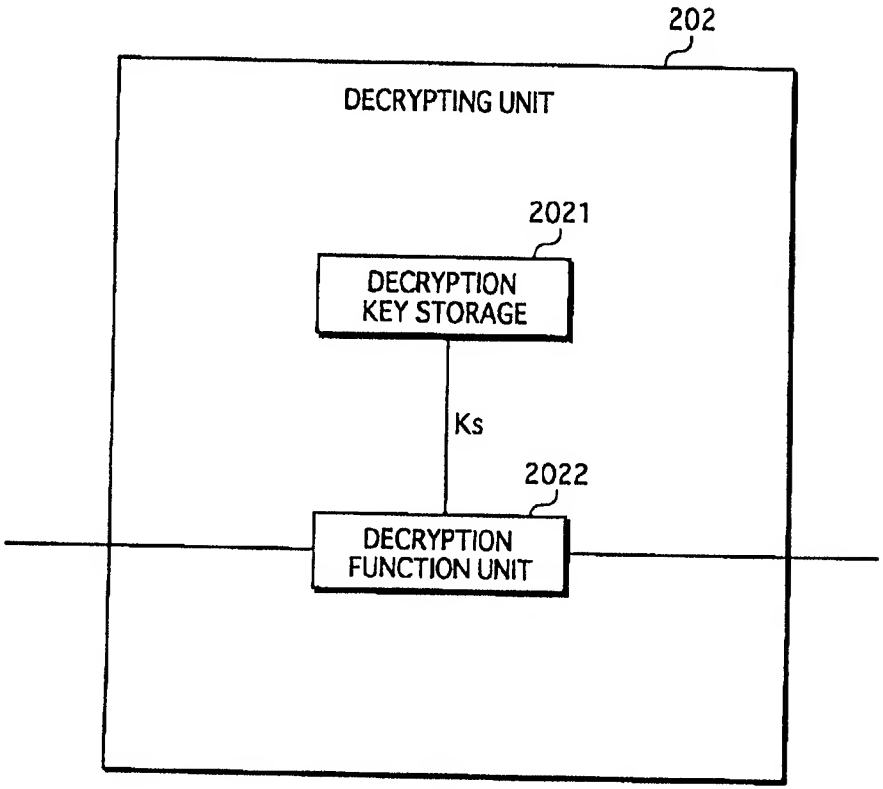

202
DECRYPTING UNIT
2021
DECRYPTION KEY STORAGE
Ks
2022
DECRYPTION FUNCTION UNIT

FIG.4

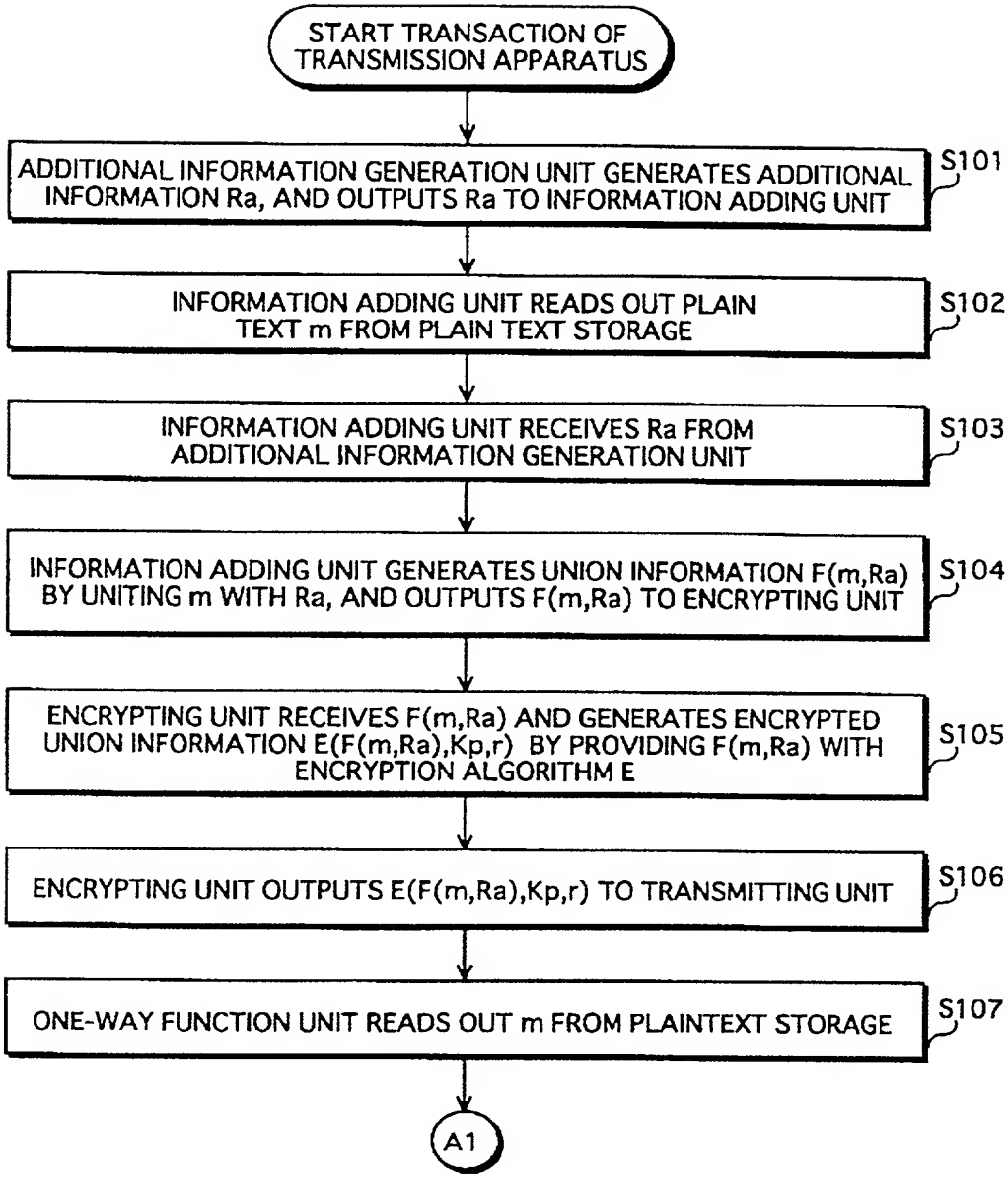

START TRANSACTION OF TRANSMISSION APPARATUS
ADDITIONAL INFORMATION GENERATION UNIT GENERATES ADDITIONAL INFORMATION Ra, AND OUTPUTS Ra TO INFORMATION ADDING UNIT
S101
INFORMATION ADDING UNIT READS OUT PLAIN TEXT m FROM PLAIN TEXT STORAGE
S102
INFORMATION ADDING UNIT RECEIVES Ra FROM ADDITIONAL INFORMATION GENERATION UNIT
S103
INFORMATION ADDING UNIT GENERATES UNION INFORMATION F(m,Ra) BY UNITING m WITH Ra, AND OUTPUTS F(m,Ra) TO ENCRYPTING UNIT
S104
ENCRYPTING UNIT RECEIVES F(m,Ra) AND GENERATES ENCRYPTED UNION INFORMATION E(F(m,Ra),Kp,r) BY PROVIDING F(m,Ra) WITH ENCRYPTION ALGORITHM E
S105
ENCRYPTING UNIT OUTPUTS E(F(m,Ra),Kp,r) TO TRANSMITTING UNIT
S106
ONE-WAY FUNCTION UNIT READS OUT m FROM PLAINTEXT STORAGE
S107
A1

Fig.5

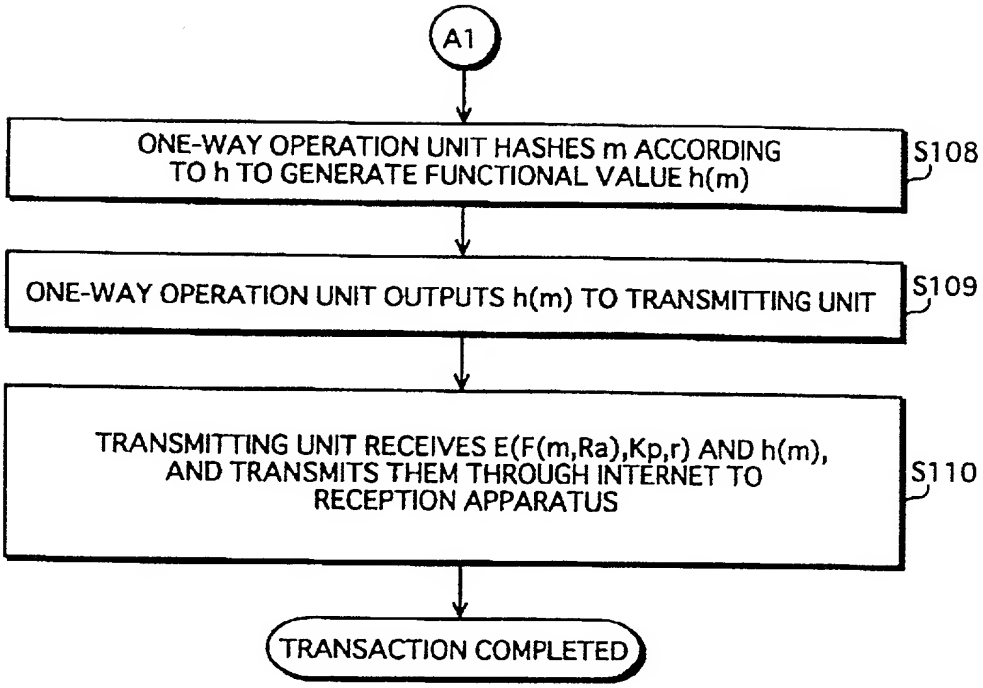
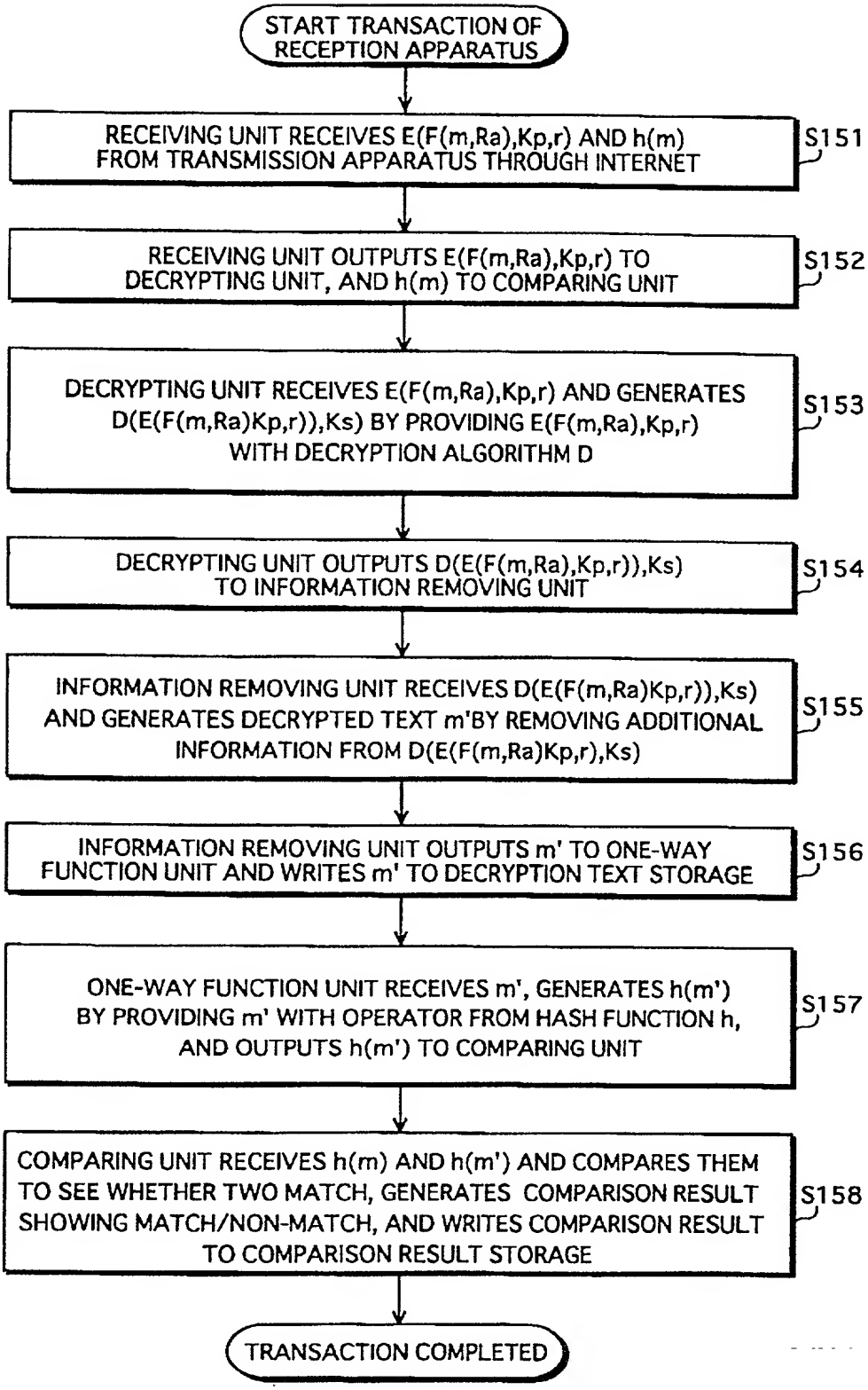

A1
ONE-WAY OPERATION UNIT HASHES m ACCORDING TO h TO GENERATE FUNCTIONAL VALUE h(m)
S108
ONE-WAY OPERATION UNIT OUTPUTS h(m) TO TRANSMITTING UNIT
S109
TRANSMITTING UNIT RECEIVES E(F(m,Ra),Kp,r) AND h(m), AND TRANSMITS THEM THROUGH INTERNET TO RECEPTION APPARATUS
S110
TRANSACTION COMPLETED

FIG.6


START TRANSACTION OF RECEPTION APPARATUS
RECEIVING UNIT RECEIVES E(F(m,Ra),Kp,r) AND h(m) FROM TRANSMISSION APPARATUS THROUGH INTERNET
S151
RECEIVING UNIT OUTPUTS E(F(m,Ra),Kp,r) TO DECRYPTING UNIT, AND h(m) TO COMPARING UNIT
S152
DECRYPTING UNIT RECEIVES E(F(m,Ra),Kp,r) AND GENERATES D(E(F(m,Ra)Kp,r)),Ks) BY PROVIDING E(F(m,Ra),Kp,r) WITH DECRYPTION ALGORITHM D
S153
DECRYPTING UNIT OUTPUTS D(E(F(m,Ra),Kp,r)),Ks) TO INFORMATION REMOVING UNIT
S154
INFORMATION REMOVING UNIT RECEIVES D(E(F(m,Ra)Kp,r)),Ks) AND GENERATES DECRYPTED TEXT m'BY REMOVING ADDITIONAL INFORMATION FROM D(E(F(m,Ra)Kp,r),Ks)
S155
INFORMATION REMOVING UNIT OUTPUTS m' TO ONE-WAY FUNCTION UNIT AND WRITES m' TO DECRYPTION TEXT STORAGE
S156
ONE-WAY FUNCTION UNIT RECEIVES m', GENERATES h(m') BY PROVIDING m' WITH OPERATOR FROM HASH FUNCTION h, AND OUTPUTS h(m') TO COMPARING UNIT
S157
COMPARING UNIT RECEIVES h(m) AND h(m') AND COMPARES THEM TO SEE WHETHER TWO MATCH, GENERATES COMPARISON RESULT SHOWING MATCH/NON-MATCH, AND WRITES COMPARISON RESULT TO COMPARISON RESULT STORAGE
S158
TRANSACTION COMPLETED

EP 0 871 321 A2

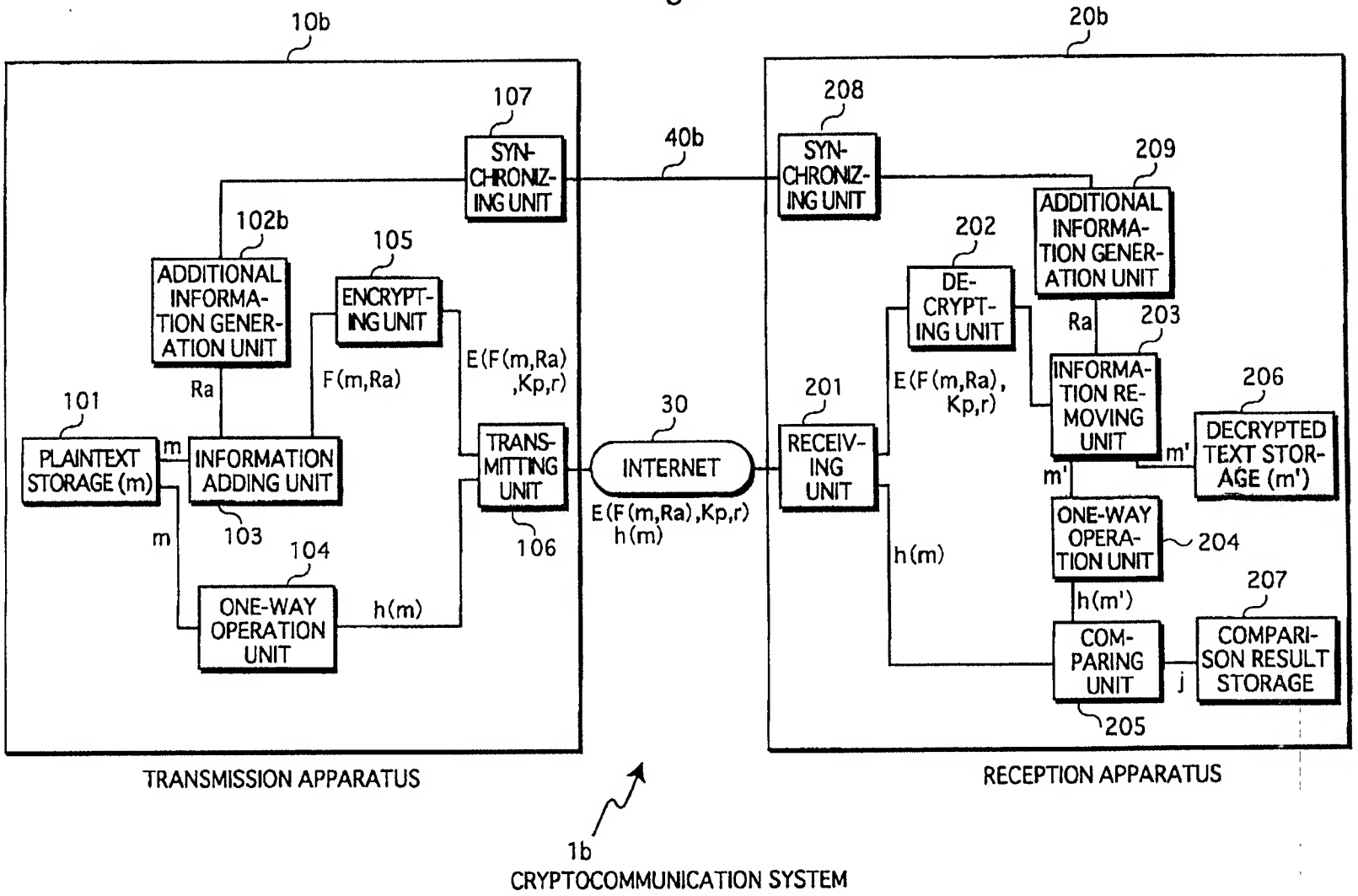
Fig.7

CONVERSION TABLE

INPUT VALUE m	OUTPUT VALUE Tab[Ra](m)
0	122
1	39
•	•
•	•
•	•
•	•
•	•
255	91

EP 1 887 730 A1

Fig.8



JP2004-080201

Fig.9

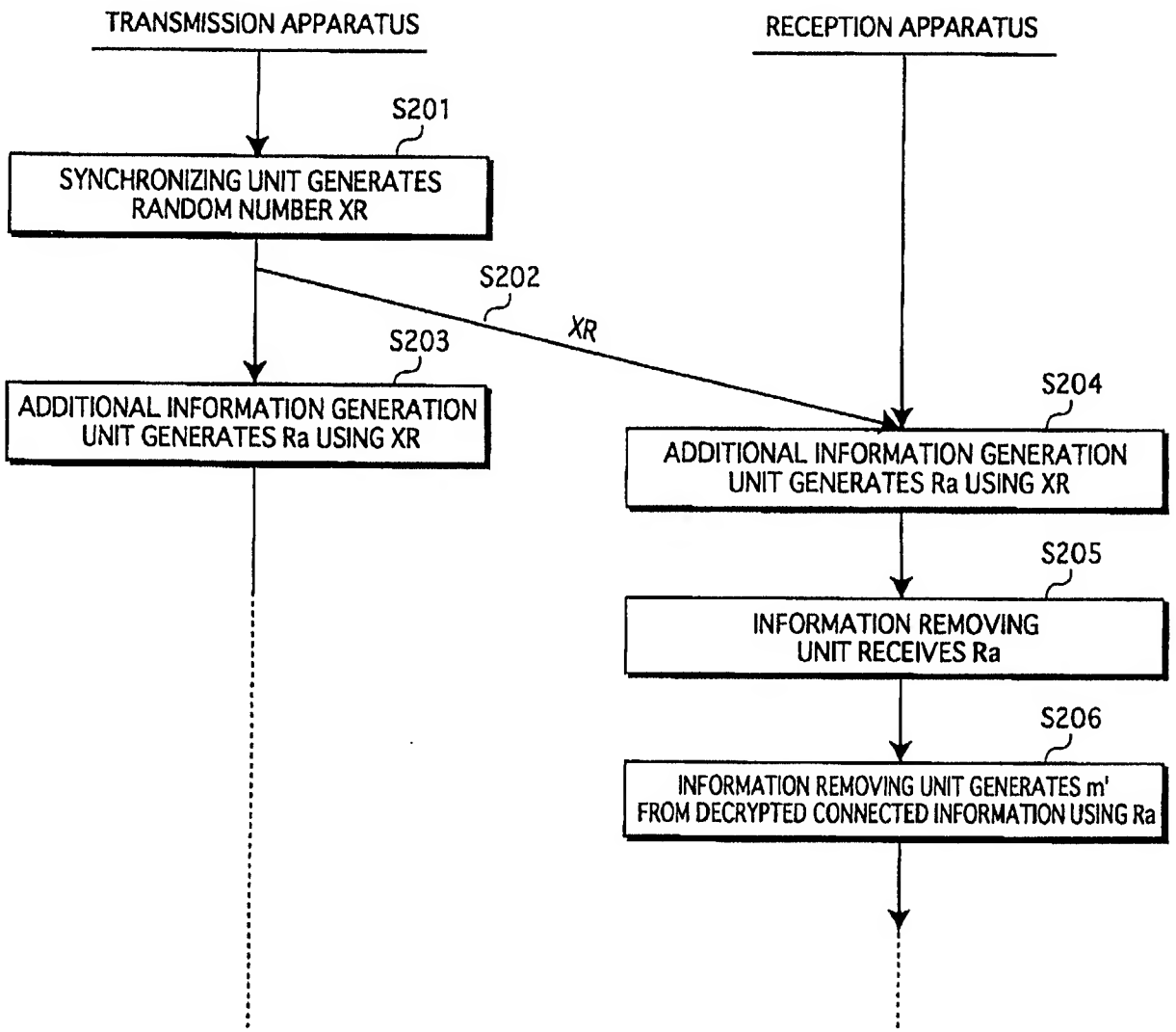


Fig.10

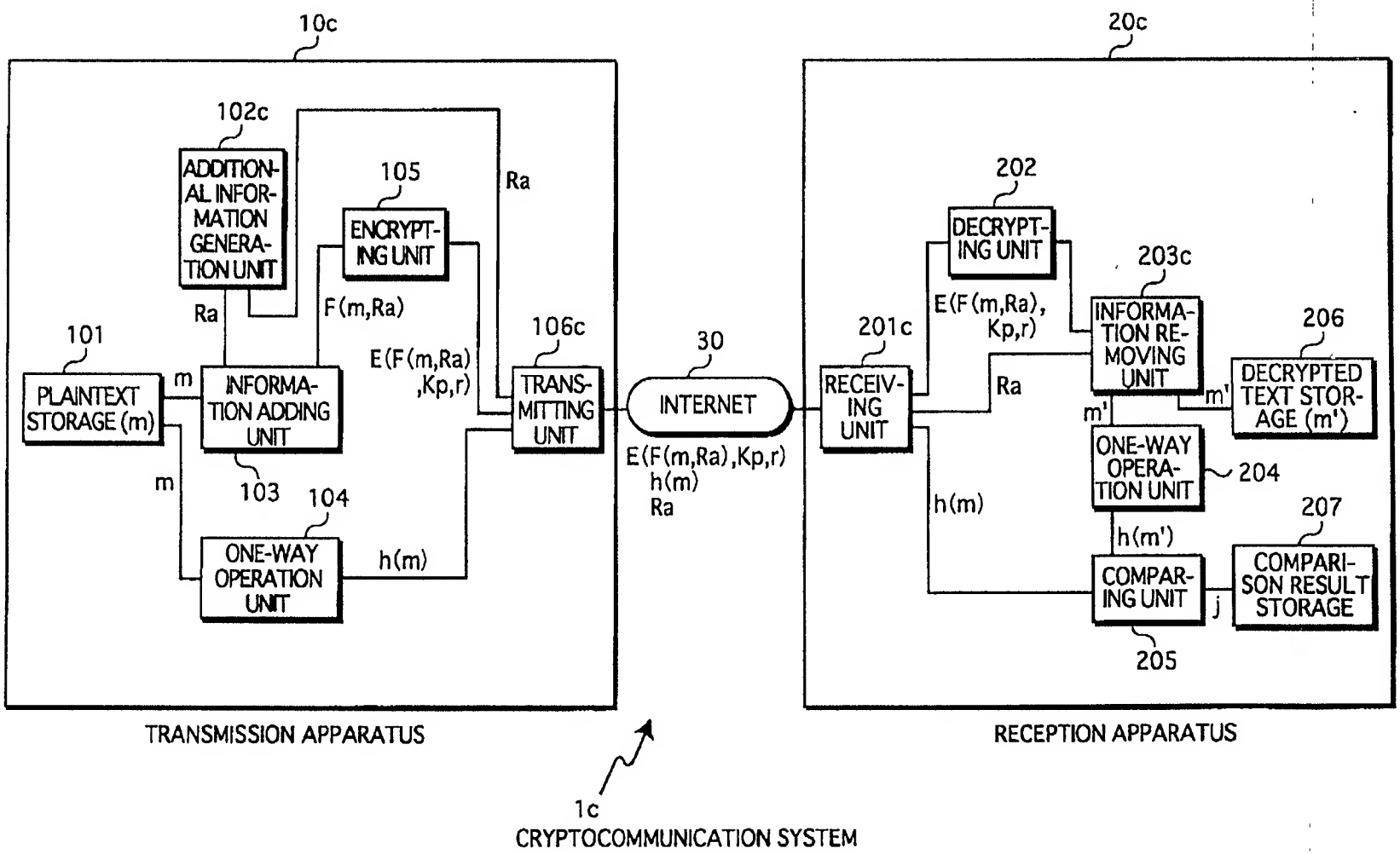

10c
20c
102c
ADDITIONAL INFORMATION GENERATION UNIT
105
ENCRYPTING UNIT
Ra
F(m,Ra)
101
PLAINTEXT STORAGE (m)
m
INFORMATION ADDING UNIT
E(F(m,Ra),Kp,r)
106c
TRANSMITTING UNIT
30
INTERNET
E(F(m,Ra),Kp,r)
h(m)
Ra
103
104
ONE-WAY OPERATION UNIT
h(m)
202
DECRYPTING UNIT
E(F(m,Ra),Kp,r)
201c
RECEIVING UNIT
Ra
h(m)
203c
INFORMATION REMOVING UNIT
m'
206
DECRYPTED TEXT STORAGE (m')
ONE-WAY OPERATION UNIT
204
h(m')
207
COMPARING UNIT
j
COMPARISON RESULT STORAGE
205
TRANSMISSION APPARATUS
RECEPTION APPARATUS
1c
CRYPTOCOMMUNICATION SYSTEM

Fig.11

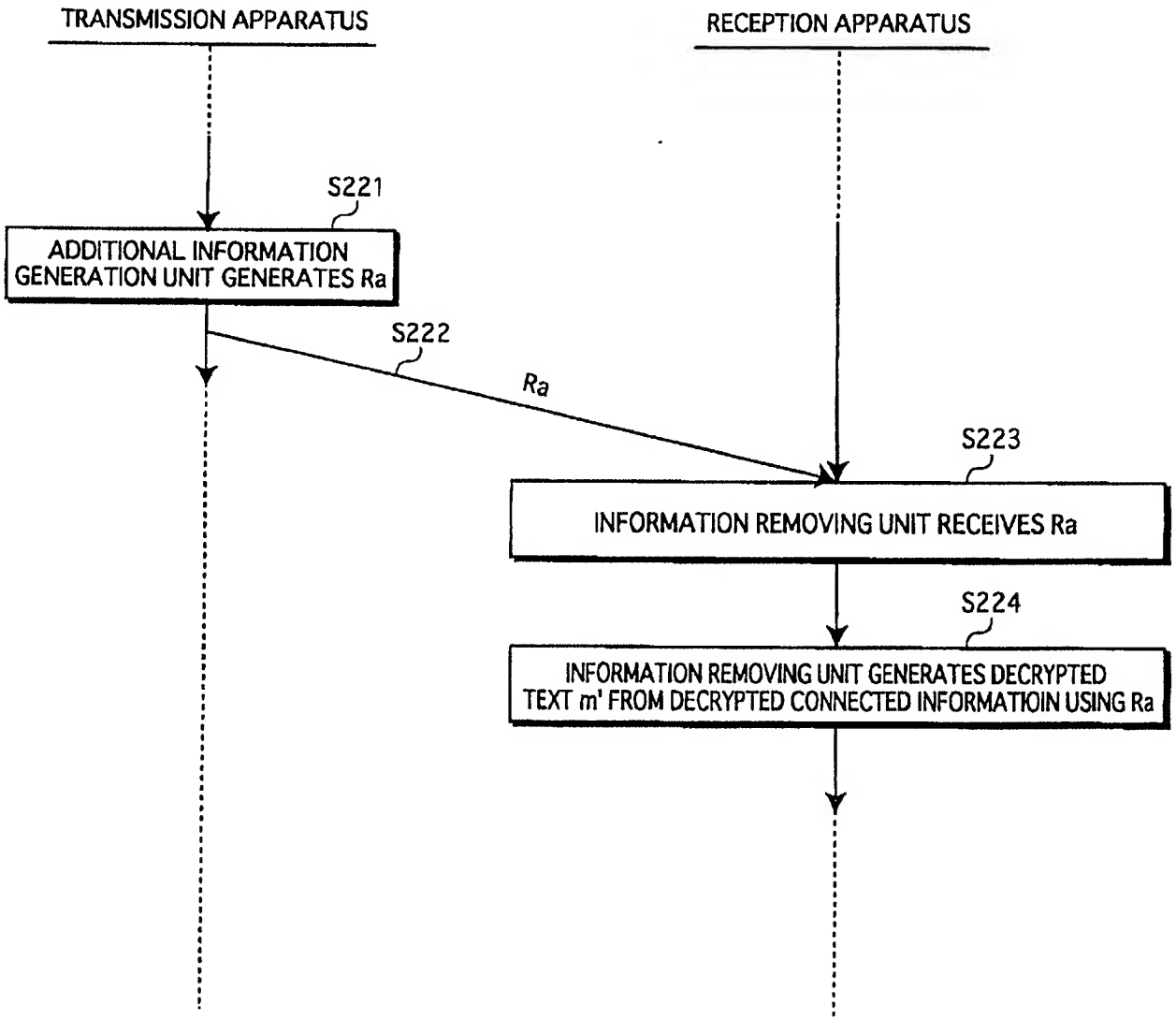
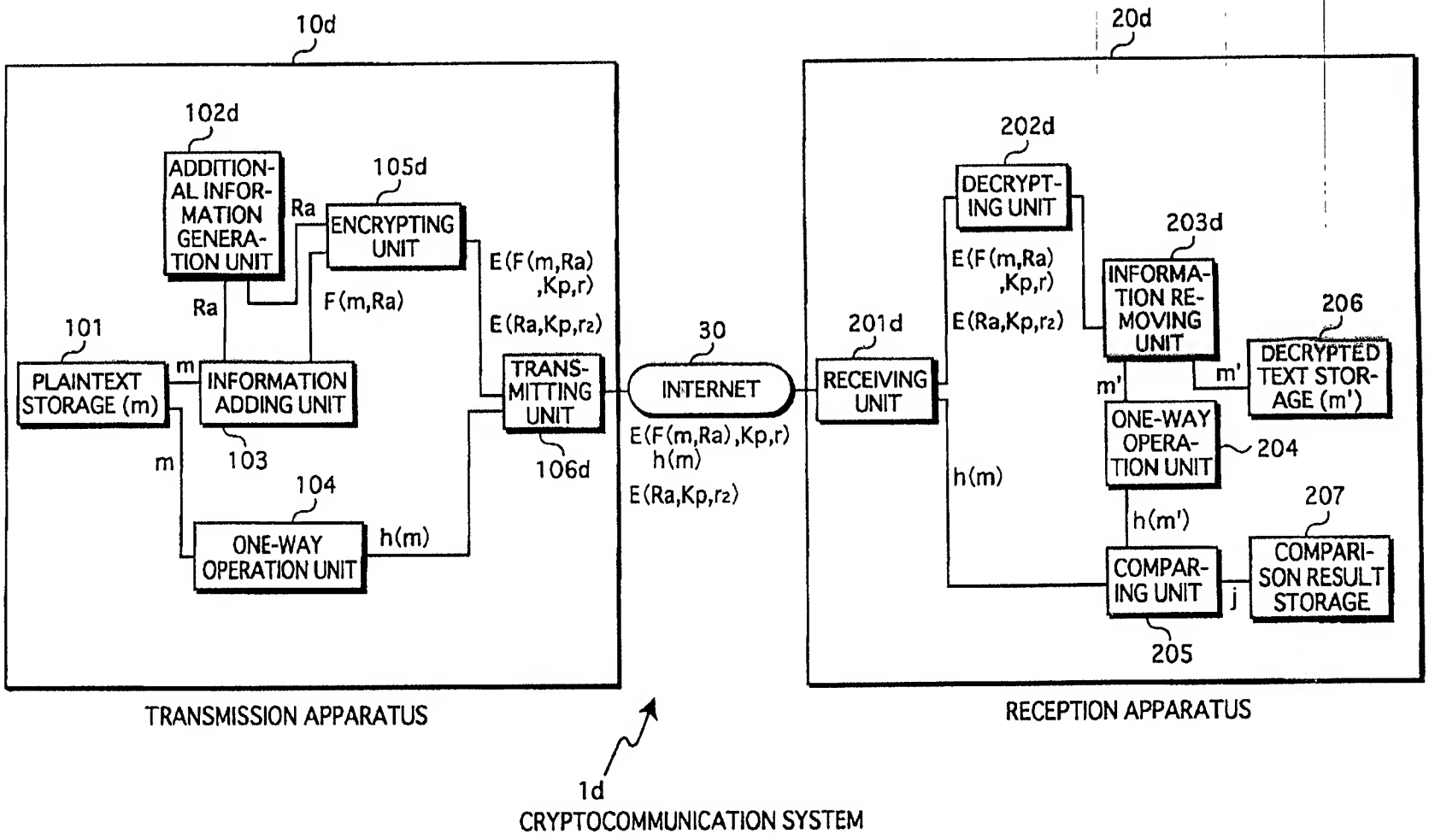

TRANSMISSION APPARATUS
RECEPTION APPARATUS
S221
ADDITIONAL INFORMATION GENERATION UNIT GENERATES Ra
S222
Ra
S223
INFORMATION REMOVING UNIT RECEIVES Ra
S224
INFORMATION REMOVING UNIT GENERATES DECRYPTED TEXT m' FROM DECRYPTED CONNECTED INFORMATIOIN USING Ra

Fig.12


10d
102d
ADDITIONAL INFORMATION GENERATION UNIT
105d
ENCRYPTING UNIT
Ra
Ra
F(m,Ra)
E(F(m,Ra),Kp,r)
E(Ra,Kp,r2)
101
PLAINTEXT STORAGE (m)
m
INFORMATION ADDING UNIT
103
m
104
ONE-WAY OPERATION UNIT
h(m)
TRANSMITTING UNIT
106d
30
INTERNET
E(F(m,Ra),Kp,r)
h(m)
E(Ra,Kp,r2)
TRANSMISSION APPARATUS
20d
201d
RECEIVING UNIT
202d
DECRYPTING UNIT
E(F(m,Ra),Kp,r)
E(Ra,Kp,r2)
h(m)
203d
INFORMATION REMOVING UNIT
m'
m'
206
DECRYPTED TEXT STORAGE (m')
ONE-WAY OPERATION UNIT
204
h(m')
207
COMPARING UNIT
205
j
COMPARISON RESULT STORAGE
RECEPTION APPARATUS
1d
CRYPTOCOMMUNICATION SYSTEM

EP 0 872 821 A2

Fig.13

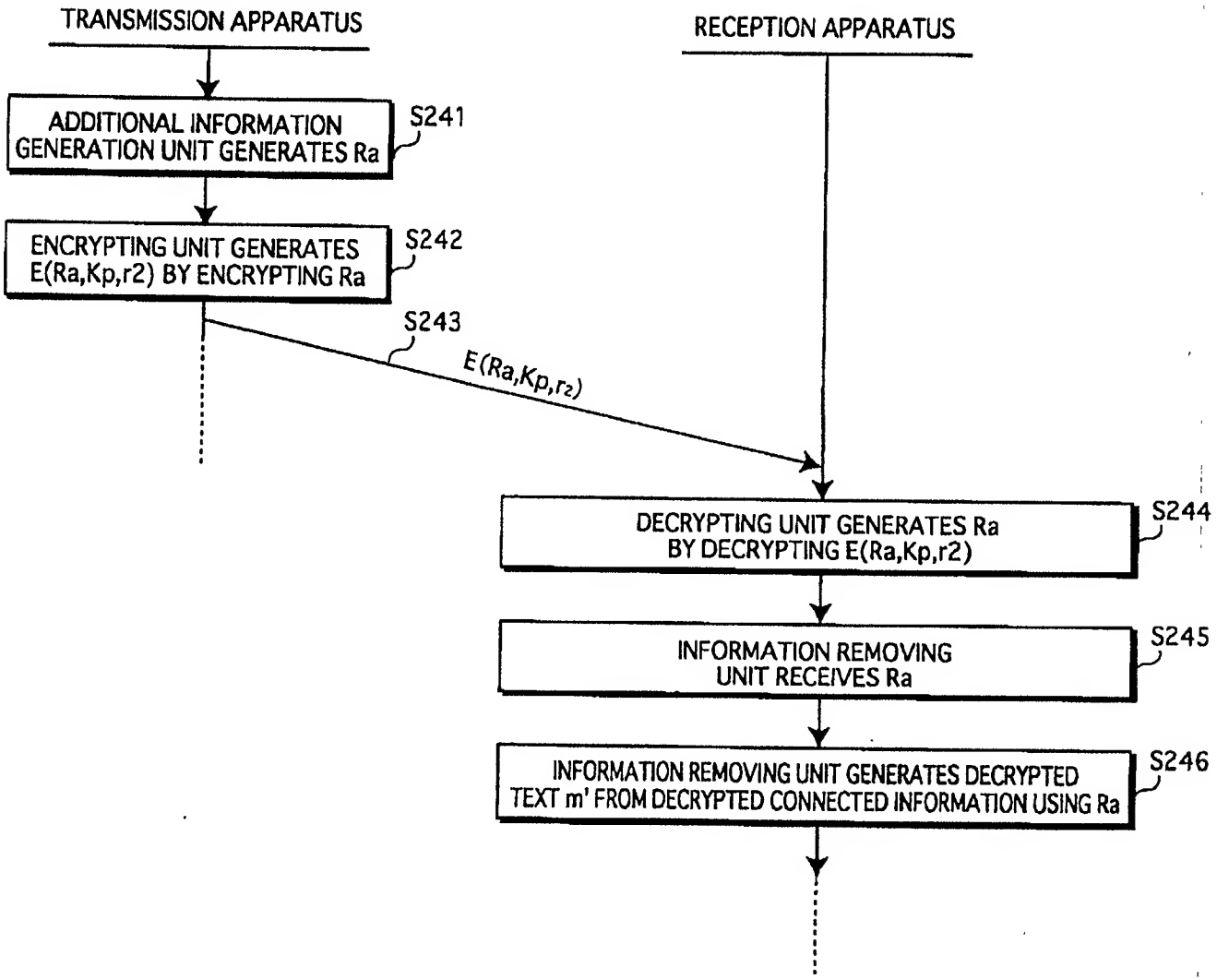


Fig.14

ADDITIONAL INFORMATION / INVERTIBLE CONVERSION F(m,Ra)	(1)Ra: RANDOM NUMBER	(2)Ra: TIME STAMP	(3)Ra: COUNTER
(1) m‖Ra	CRYPTOCOMMUNICATION SYSTEM 1,1b~1d		
(2) m⊕Ra	CRYPTOCOMMUNICATION SYSTEM 1b~1d		
(3) m+Ra			
(4) m×Ra mod p			
(5) BitPerm[Ra](m)			
(6) Tab[Ra](m)			